

MaxPatrol VM

pt



Михаил Козлов,
руководитель продукта
MaxPatrol VM



Павел Попов,
Лидер практики по
управлению уязвимостями

**Управление уязвимостями
с MaxPatrol VM: инструкция
по применению**

Что такое процесс?



Управление уязвимостями

VM



01

Следим за постоянной актуализацией данных об активах



03

Договариваемся с IT и фиксируем политики



05

Следим за устранением уязвимостей и за соблюдением политик



02

Оцениваем и классифицируем активы



04

Система определяет и сортирует уязвимости



06

Смотрим общие метрики, оцениваем тренд по компании



Asset management
Управление активами



Выделение особо опасных уязвимостей.

Оперативное реагирование на них **вне процесса.**

Процесс управления активами

Управление активами (asset management, AM) — процесс, в ходе которого выполняется формирование подробной картины IT-инфраструктуры организации, отражаемой в базе активов MaxPatrol VM, а также поддержка сведений об активах в актуальном состоянии.

Почему процесс AM важен

1. Обнаруживает активы, по которым не проводилось сканирование
2. Помогает приоритизировать сроки устранения уязвимостей (важна не только степень критичности уязвимости)
3. Повышает качество мониторинга за счет того, что предоставляет полные и актуальные сведения об активах

УПРАВЛЕНИЕ АКТИВАМИ
Инвентаризация и контроль

ВХОДНЫЕ ПАРАМЕТРЫ

- Количество и группы активов
- Уровень значимости активов
- Сведения о новых и выведенных из эксплуатации активах

Управление уязвимостями

- Выявление уязвимостей
- Анализ и приоритизация уязвимостей
- Устранение уязвимостей
- Контроль устранения уязвимостей

МОНИТОРИНГ СОБЫТИЙ ИБ

НА ДАННОМ ЭТАПЕ ВАЖНО ОПРЕДЕЛИТЬ

- Что это за актив
- Насколько сведения об активе являются полными
- Владельца / администратора актива
- Назначение актива — в каких бизнес-процессах компании он принимает участие

СПОСОБЫ СБОРА СВЕДЕНИЙ ОБ АКТИВАХ



ПРИМЕР №1

Смотрим, где в сети есть **Zerologon**, создаем точечный профиль с CVE-2020-1472

Создать профиль для выбранных уязвимостей

Выбрать уязвимости:

CVE, mprbid, OSVDB уязвимости или идентификатор в Knowledge Base

Порты:

Искать только на стандартных портах

Использовать список портов по умолчанию

Анализ результатов сканирования



Оценка значимости активов для бизнес-процессов компании



Классификация и распределение активов по группам для автоматизации работы

Приоритизация и группировка активов



БАЗА
АКТИВОВ



Назначение
актива понятно?

Да – группировка
активов



РЕЕСТР
ЦЕЛЕВЫХ И
КЛЮЧЕВЫХ
СИСТЕМ



АДМИНИСТРАТОР
АКТИВА

Нет –
уточнение
информации

Целевая система

AD

СУБД

АРМ

Другие

UnixHost

WindowsHost

Сетевое устройство

Другие

Классификация и оценка активов

Классификация активов

- Динамические группы
- Статические группы
- Триггеры для контроля изменений состава групп

Распределение активов по группам

- По принадлежности к структурным подразделениям
- По принадлежности к АС
- По принадлежности к IP-сетям
- По наличию определенных ОС и ПО

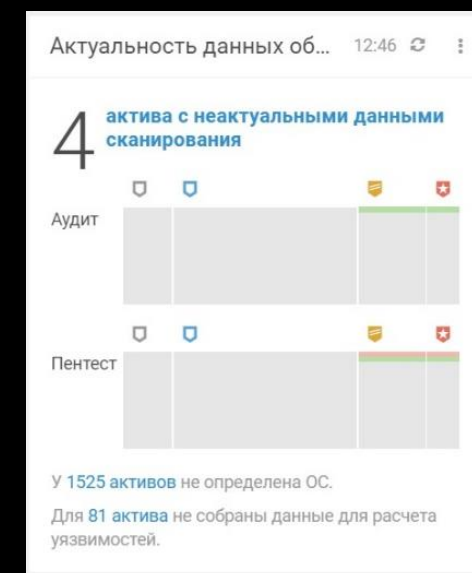
Контроль активов

их классификации, оценка регулярности сканирования и устаревания

Оценка активов

задание степени важности

MaxPatrol VM



ПРИМЕР №2

Задаем всем контроллерам домена высокую значимость

The screenshot shows the MaxPatrol 10 interface. The top navigation bar includes 'Активы', 'Инциденты', 'Сбор данных', and 'Система'. The main area displays a query titled 'Запрос: Критически важные роли на базе Windows'. The query is: `WindowsHost.HostRoles.Role in ['Domain...'] | @WindowsHost, WindowsHost.OsName as 0...`. Below the query is a table with the following columns: Узел, Операционная система, Виртуальное устройство, Тип узла, DomainRole, Роль, and Список IP-адресов.

Узел	Операционная система	Виртуальное устройство	Тип узла	DomainRole	Роль	Список IP-адресов
@WindowsHost	OsName	isVirtual	HostType	DomainRole	Role	IpList
srv10.company.com (192.168.2.15)	Windows 2012 R2	True	Server	Read-Write Doma...	DHCP Server	::1 127.0.0.1 1...
srv10.company.com (192.168.2.15)	Windows 2012 R2	True	Server	Read-Write Doma...	Directory Service	::1 127.0.0.1 1...
srv10.company.com (192.168.2.15)	Windows 2012 R2	True	Server	Read-Write Doma...	DNS Server	::1 127.0.0.1 1...
srv10.company.com (192.168.2.15)	Windows 2012 R2	True	Server	Read-Write Doma...	Domain Controller	::1 127.0.0.1 1...
srv10.company.com (192.168.2.15)	Windows 2012 R2	True	Server	Read-Write Doma...	Web Server	::1 127.0.0.1 1...

ПРИМЕР №3

Находим нелегитимное или устаревшее ПО

MaxPatrol 10 | Активы | Инциденты | Сбор данных | Система

Активы | Все активы

Запрос: ПО Windows, группировка по версии *

WindowsHost.Softs | @WindowsHost, WindowsHost.Softs.Name ... | Уникальные | @WindowsHost ASC | SoftName, SoftVersion, COUNT(*) | Выполнить

↓ SoftName ASC

Название SoftName	Версия SoftVersion	COUNT(*)	Узел @WindowsHost	Название SoftName	Версия SoftVersion	Дата и время последнего обновления акт... WindowsHost.UpdateTime
TeamViewer	10.0.47484	1	pc8.company.com (192.168.0.94)	TeamViewer	10.0.47484	15 марта, 00:29
TeamViewer	15.6.7	1				
Thunderbird	38.3.0	1				
Tor	Tor	1				
Tor Browser	5.0.3	1				

Процесс управления уязвимостями



Управление уязвимостями (Vulnerability Management, VM) — процесс, в ходе которого выполняется сканирование инфраструктуры на предмет наличия известных уязвимостей, приоритизация уязвимостей, информирование о выявленных уязвимостях, подготовка предложений по их устранению и контроль устранения

Решаемые задачи:

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ

Анализ информации о существующих и потенциальных уязвимостях

ОЦЕНКА ОПАСНОСТИ УЯЗВИМОСТЕЙ

Анализ и оценка влияния уязвимостей на защищенность компании

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

Оперативное принятие мер по устранению уязвимостей

ВЫСТРАИВАНИЕ ПРОЗРАЧНЫХ ОТНОШЕНИЙ С IT-ОТДЕЛОМ

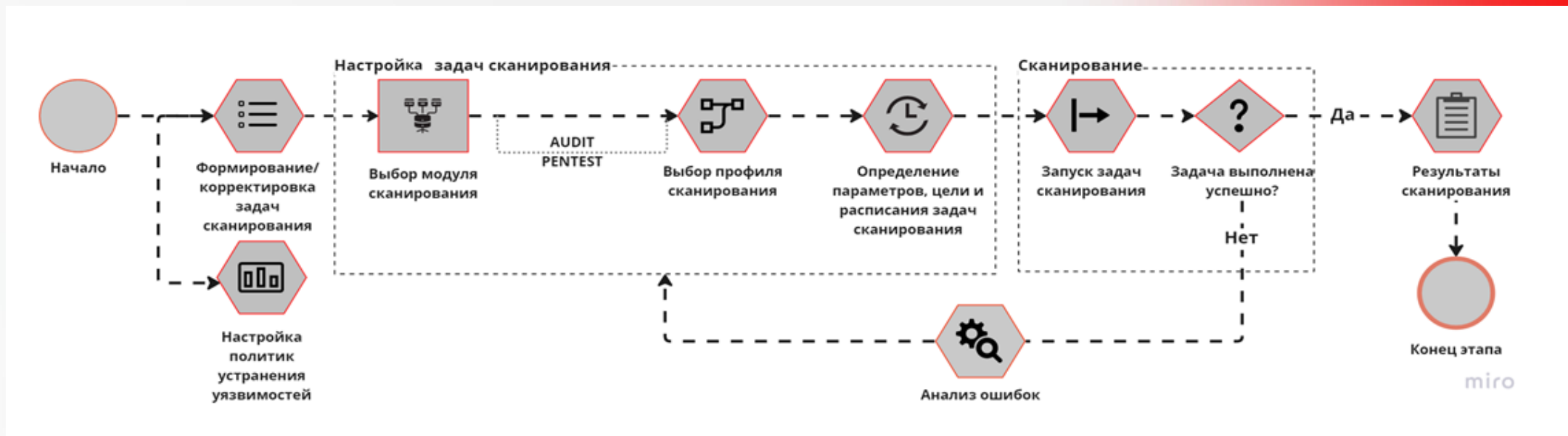
Фиксация достигнутых договоренностей

КОНТРОЛЬ УСТРАНЕНИЯ

Своевременный контроль защищенности компании

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА

Постоянное улучшение процесса VM



Источники данных об уязвимостях

- Сведения об уязвимостях от разработчиков СЗИ, общесистемного, прикладного и специального ПО, ТС
- Общедоступные источники данных об уязвимостях (MITRE CVE, OSVDB, БДУ ФСТЭК России)

Параметры сканирования

- Периодичность сканирования
- Перечень активов для сканирования
- Профили сканирования

Рекомендации

- Процесс выявления уязвимостей должен быть постоянным, структурированным и охватывать всю ИТ-инфраструктуру
- Фокус на трендовые уязвимости

Классификация и приоритизация уязвимостей

Задание политик

- Для планового устранения уязвимостей специалистами IT

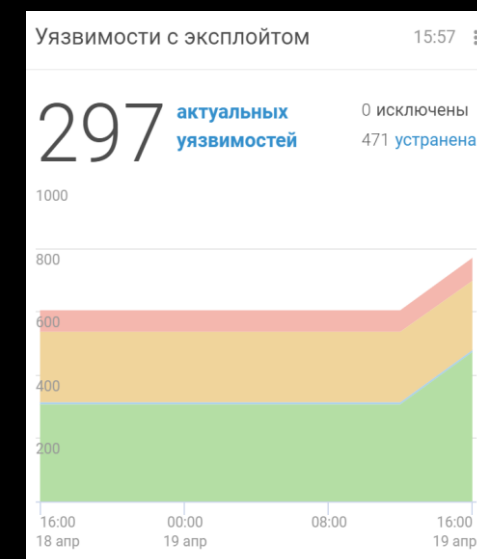
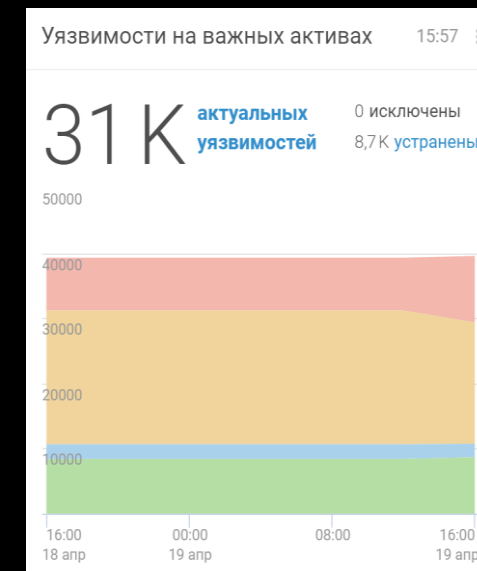
Фильтрация уязвимостей при ручном разборе

- Активы особой важности
- Уязвимости, непокрытые политиками
- Неустраняемые уязвимости (с техническими ограничениями)
- 0-day

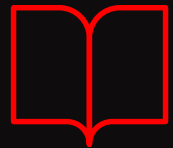
Контроль особо опасных уязвимостей

Выделяем наиболее критичные уязвимости для инфраструктуры

MaxPatrol VM



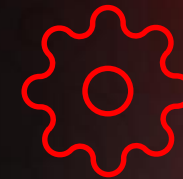
Выявляет уязвимости без сканирования



Хранит полную
информацию
об активах
и историю
изменений



Определяет активы,
используя сведения из
внешних источников



Актуализирует
информацию
об уязвимостях
автоматически
после обновления
базы знаний

Выявления уязвимостей без повторного сканирования

Информация об уязвимостях актуализируется автоматически после обновления базы знаний



5 уведомлений ⚙️ Настройка ✕ Удалить все

14 апреля ✕

- ! Перерасчет уязвимостей завершен
Данные об уязвимостях на активах актуальны 09:20
- ! Идет перерасчет уязвимостей
До завершения перерасчета данные об уязвимостях на активах могут быть неактуальными 09:18
- ! База знаний обновлена до ревизии 353141 09:18
- ! База знаний обновляется до ревизии 353141 09:08

Устранение уязвимостей

СПОСОБЫ УСТРАНЕНИЯ

Обновления

Компенсирующие меры

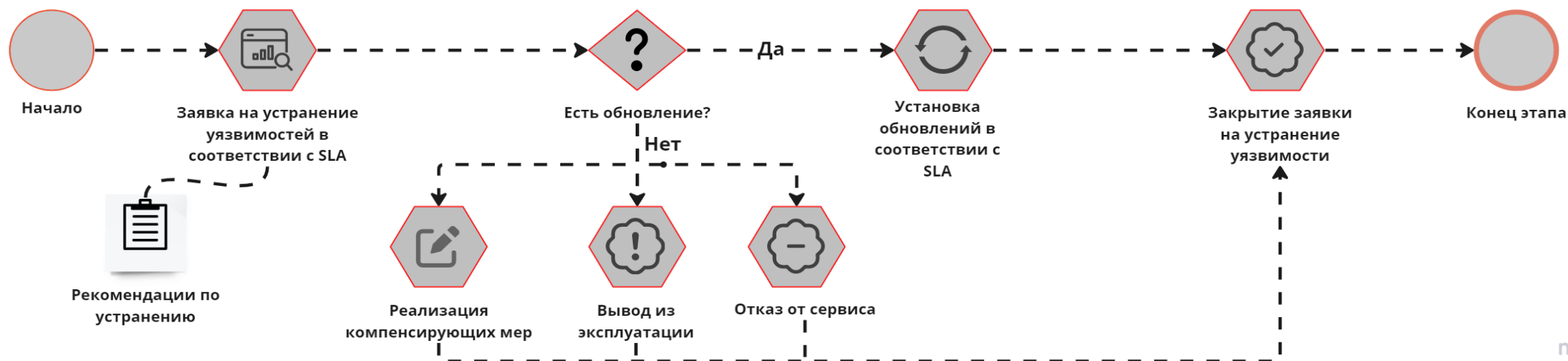
Отказ от сервиса

Плановое обновление

- ИТ устраняет уязвимости в рамках планового обновления ПО
- ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с ИТ

Внеплановое обновление

- Фокус смещается на трендовые уязвимости и те, что имеют эксплоит и расположены на важных активах
- О сроках устранения каждой уязвимости ИБ и ИТ договариваются отдельно



Трендовые уязвимости



MaxPatrol VM регулярно поставляет информацию о самых опасных уязвимостях, которые злоумышленники эксплуатируют прямо сейчас.



Опыт и знания
специалистов
Positive
Technologies

- Пентесты
- Исследование угроз
- Расследование инцидентов ИБ



PT
Knowledge
Base

- Способы выявления и устранения уязвимостей
- Бюллетени безопасности



MaxPatrol VM

- Выявление уязвимостей
- Выделение трендовых уязвимостей
- Рекомендации по их устранению

Трендовые уязвимости

Популярны у злоумышленников и их нужно устранить в первую очередь.
В MaxPatrol VM 2.0 реализована доставка информации о трендовых уязвимостях за 12 часов!

Трендовые уязвимости 11:00 ⋮

31 августа

■ **Уязвимость CVE-2023-21707** CVE-2023-21707 Уязвимости не обнаружены

Уязвимость в Microsoft Exchange Server, связанная с небезопасной десериализацией, позволяющая злоумышленнику удаленно выполнить код на системе. Уязвимость может быть использована для...

25 августа

■ **Уязвимость CVE-2023-38831** CVE-2023-38831 Уязвимости не обнаружены

Уязвимость в Winrar, позволяющая замаскировать один тип файла под другой, и используемая для доставки вредоносного ПО. Софт крайне сильно распространен и установлен на почти каждом Windows...

■ **Уязвимость CVE-2023-40477** CVE-2023-40477 Уязвимости не обнаружены

Уязвимость выход за границы массива в RARLAB WinRAR. Злоумышленник, успешно проэксплуатировавший уязвимость, получает возможность выполнения произвольного кода от имени...

21 июня

Трендовые уязвимости на активах 17:00 ⋮

Актуальные

<p>Активы высокой значи... Остальные активы</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #e6f2ff;"> <p style="font-size: 2em; font-weight: bold;">247</p> <p style="text-align: right; font-size: 0.8em;">12</p> <div style="width: 100%; height: 10px; background-color: #007bff; margin-bottom: 5px;"></div> <p style="font-size: 0.8em;">247 И</p> </div>	<div style="border: 1px solid #ccc; padding: 10px; background-color: #fff9c4;"> <p style="font-size: 2em; font-weight: bold;">146</p> <p style="text-align: right; font-size: 0.8em;">7</p> <div style="width: 100%; height: 10px; background-color: #ffc107; margin-bottom: 5px;"></div> <p style="font-size: 0.8em;">2 Н 144 И</p> </div>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Исправленные

<p>Исключенные Устраненные</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #e6e6e6;"> <p style="font-size: 2em; font-weight: bold;">0</p> <p style="text-align: right; font-size: 0.8em;">0</p> <div style="width: 100%; height: 10px; background-color: #6c757d; margin-bottom: 5px;"></div> <p style="font-size: 0.8em;">0 И</p> </div>	<div style="border: 1px solid #ccc; padding: 10px; background-color: #e6ffe6;"> <p style="font-size: 2em; font-weight: bold;">0</p> <p style="text-align: right; font-size: 0.8em;">0</p> <div style="width: 100%; height: 10px; background-color: #28a745; margin-bottom: 5px;"></div> <p style="font-size: 0.8em;">0 У</p> </div>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Контроль устранения

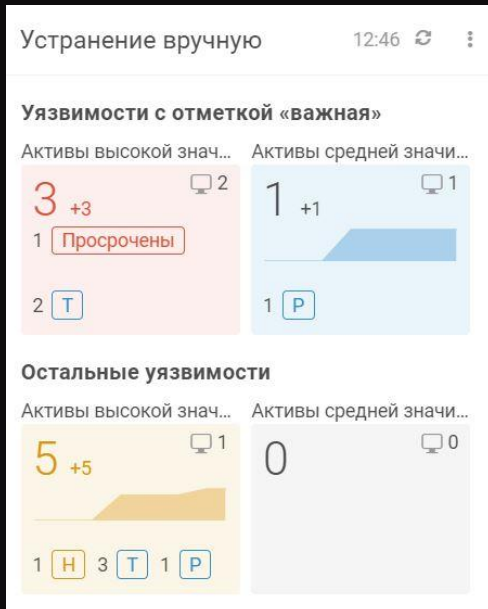


Контроль устранения уязвимостей вручную

Целевое состояние



Контроль устранения уязвимостей автоматизирован



Оценка соблюдения политик и устранения уязвимостей

Задание **сроков устранения уязвимостей** в зависимости от их типа и важности активов

Отслеживание динамики наличия **просроченных уязвимостей**, отдельная статистика по ООУ

Анализ устранения уязвимостей позволяет понять, нужные ли уязвимости устранялись и на тех ли активах велись работы



Комплаенс-контроль



Экспертиза
Positive
Technologies

Возможности

MaxPatrol VM

База знаний
об уязвимостях

Построение процесса
управления уязвимостями

- Обнаружение и приоритизация уязвимостей
- Контроль выявления и устранения уязвимостей



MaxPatrol HCC

Пакеты
стандартов

Построение процесса
комплаенс-контроля

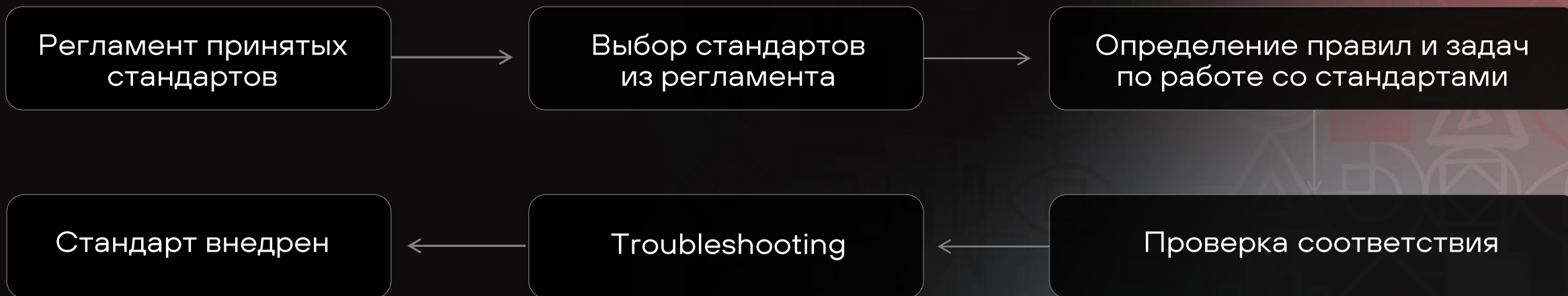
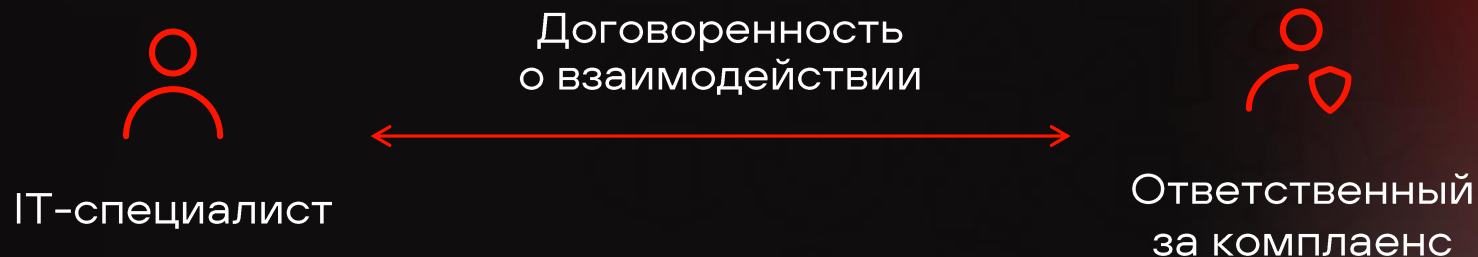
- Использование экспертных стандартов
- Возможность создавать свои критерии проверки

Основа

Security asset management

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

Внедрение стандартов



Регулярный контроль соответствия стандартам



Ответственный
за комплаенс

Проверка активов
на соответствие
стандартам

Работа с отчетом
о нарушении стандартов



IT-специалист

Подготовка новых стандартов
и модификация существующих
совместно со специалистом
по комплаенсу



Руководитель
отдела ИБ

Роль MaxPatrol VM в построении процесса



Этап процесса

MaxPatrol VM



1. ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

Требуется глубокая проверка IT-инфраструктуры, выявление уязвимостей компонентов и ошибки в их конфигурации



- Сканирует IT-инфраструктуру и собирает информацию по 3000 и более параметров
- Выявляет версионные и конфигурационные ошибки



2. АНАЛИЗ И ПРИОРИТИЗАЦИЯ

Требуется структурировать информацию о выявленных уязвимостях для более эффективного взаимодействия команд ИБ и ИТ



- Использует правила обработки уязвимостей
- Контролирует соблюдение политик для отслеживания SLA по устранению уязвимостей



3. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

Требуется упростить и автоматизировать процесс устранения



- Учитывает принятые компенсирующие меры
- Позволяет настроить исключение уязвимостей
- Передает в ИТ отчет о трендовых уязвимостях



4. КОНТРОЛЬ УСТРАНЕНИЯ

Требуется обеспечить мониторинг устранения уязвимостей без лишних заявок в ИТ



- Автоматически проверяет устранение уязвимостей по расписанию
- Обладает настраиваемыми виджетами для отслеживания устранения уязвимостей
- Выполняет точечные проверки для контроля устранения

Чек-лист для работы с уязвимостями



1

Согласован SLA на патч-менеджмент

2

Есть плановая и ручная обработка уязвимостей

3

Задан критерий для определения важных уязвимостей

4

Количество просроченных уязвимостей
минимизировано

5

Просроченные уязвимости устраняются быстро

Курс-практикум «Как управлять уязвимостями»

Старт 22 октября

Регистрация и первый
бесплатный модуль



4

недели
обучения

Каждую неделю
новый тематический
блок с теорией,
практическим
заданием и тестом
для проверки знаний



12

часов общения
с экспертами

Каждое воскресенье
с 11 до 14 часов
воркшопы
с экспертами,
на которых
участники могут
задать вопросы

16

часов
онлайн

Можно заниматься
в удобное время

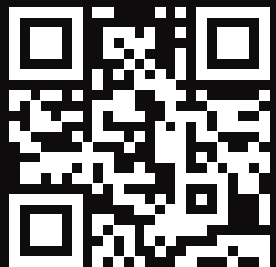
8

часов
практики

Доступ
к тренировочному
стенду MaxPatrol VM,
участники курса
решают типовые
задачи управления
уязвимостями



Присоединяйтесь к Позитиву



Читайте нас на Хабр
[habrahabr.ru/
company/pt](https://habrahabr.ru/company/pt)



**Узнавайте все про
наши продукты**
t.me/ptproductupdate



**Присоединяйтесь к
чату продукта**
<https://t.me/MPSIEMChat>



**Регистрируйтесь на
курс по управлению
уязвимостями**
<https://vm.edu.ptsecurity.com>